Set of Components/Component Safety Data (acc. IEC 61508)

Set of Components/Component	**Lined Butterfly Valves** **Series XLD**	
Manufacturer	XOMOX International GmbH & Co.OHG	
Component Type	Type A	Ref. IEC 61508-2
Mode of Operation	Low demand operation	
Safety Function, SF1	Valve closing, within specified safety time.	
Safe State, SS1	Valve closed, with specified leakage rate.	
Safety Function, SF2	Valve opening, within specified safety time.	
Safe State, SS2	Valve opened, with specified mass flow rate.	

Failure Rates by FMEDA [failure/10^9 hrs = FIT]

Failure Rate Distribution	λ_{total}	λ_{safe}	$\lambda_{dangerous\ detected}$	$\lambda_{dangerous\ undetected}$	$\lambda_{don't\ care}$	SFF [%]
SUM (with diagnostic test)	38	0	23	**15**	61	61
SUM (without diagnostic test)			0	**38**		0

Specification of component Architecture

Architecture	**1oo1**	is the architecture of a single set of components/component of the analyzed type.
Hardware Fault Tolerance HFT	**0**	Due to HFT=0, one failure has impact on the safety function of a single set of components/component of the analyzed type.
MTTR / MRT	**32 h / 8 h**	MTTR is the time required to detect and for repair of the component in case of failure. MRT is the time required for repair of the component. MTTR/MRT has marginal influence on the pfd-value. MRT is exemplary, deviating MRT must be considered in pfd-calculation.
Diagnostic Test	**PST**	Diagnostic test used to detect dangerous failures during operation. PST: Partial Stroke Test, valves with actuator in open/close application is moved out of activated position. Movement is recognized by a binary sensor (moved / not moved). Valve must leave activated position within a specified time frame. For valves in control applications, position is monitored during control process by continuous comparison of specified and actual valve position.
Diagnostic Coverage (DC)	**61 %**	In case of missing automatic diagnosis: DC = 0 %. In case of implemented diagnostics: DC > 0% (value depends on efficiency of diagnosis). Safe Failure Fraction SFF increased by higher DC.
Diagnostic Test Interval	**24 h**	Max. diagnostic test interval to perform online diagnostics to detect potential dangerous failures during operation amounts to 24 h. Deviating diagnostic test interval must be considered in pfd-calculation, by deviating MTTR.
Beta Factor	**β_{int} = 5%** β_{Dint} = 2%	Beta factor, which has to be considered if the components/component are used in safety relevant architectures with a HFT ≥ 1. Detailed beta factor has to be calculated for each individual application. The beta factor depends on the exact architecture where the components/component is used in. See IEC 61508-6, table D.5 how to calculate beta factor.

Verification of SIL Capability (examples considering diagnostic test)

(see comments on next page/backside of this page)

Proof Test Interval	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFDavg (IEC 61508-6, B.3.2.2; λ_{du} from FMEDA)	6.66 E-05	1.32 E-04	1.98 E-04	2.64 E-04	3.29 E-04
Single component application (**HFT = 0)** Max. achievable SIL acc. IEC 61508-1, table 2 and IEC 61508-2, 7.4.4.2, Route 1_H	**SIL 2**				
Redundant component application (**HFT ≥ 1**) Max. achievable SIL acc. IEC 61508-1, table 2 and IEC 61508-2, 7.4.4.2, Route 1_H	**SIL 3**				

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöring	Pöring, 2022-12-22	

Explanations to the Data Sheet

The data sheet is divided in 4 areas:

- Common technical description of the set of components/component (blue)
- Failure rates (light green)
- Specification of architecture of the set of components/component (light orange)
- Verification of SIL capability (examples) (grey)

General description of the Part / Component:

- Information on the set of components/component, type of component and component designator
- Manufacturer information
- Component type (Type A or Type B) acc. IEC 61508-2/7.4.4.1.2 und 7.4.4.1.3)
- Mode of operation of the set of components/component (acc. IEC 61508-1)
- Description of the safety function of the set of components/component
- Description of the safe state of the set of components/component

Failure Rates and Failure Rate Distribution

The failure rates and failure rate distribution are the results of the reliability calculation of the set of components/ component and the Failure Modes Effects and Diagnostic Analysis (FMEDA). The failure rates can be used for further quantitative analysis of the set of components/component as pfd/pfh-calculation, Markov-Analysis, Fault Tree Analysis, and due to this for a quantitative evaluation of SIL-capability of the set of components/component.

Based on the failure rate distribution the Safe Failure Fraction (SFF) is calculated according the formula SFF [%] = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$.

Specification of Component Architecture

The architecture of the set of components/component is described by following parameters:

- Structure/architecture (single-channel, multi-channel expressed by 1oo1, 1oo2, 1oo3, etc.)
- Hardware-Fault-Tolerance (HFT) (number of failures acceptable without dispatch on the safety function of the set of components/component)
- Mean Repair Time (MRT): In case of inspection, the MRT is the mean repair time of the component/set of components. In general, the MRT is application specific. The user is responsible to define realistic MRT for the specific application. The MRT given in the datasheet is exemplary, deviating MRT must be considered in pfd-calculation.
- Mean Time to Repair (MTTR): Mean time to repair the set of components/component in case of detected dangerous failure. MTTR is the sum of MRT and diagnosis test interval.
- Diagnostic Coverage: The diagnostic coverage is resulting from the diagnostic test for the set of components/component in case of application of automatic diagnosis (e.g. partial stroke test). The diagnostic coverage is considered in the FMEDA and the quantitative results of the analysis (see failure rates).
- Diagnostic Test: The type of installed on-line automatic diagnostic test to detected dangerous failure during operation. The diagnostic test has to fulfill requirements acc. IEC 61508-2.
- Diagnostic Test Interval: Interval between diagnostic tests to detect dangerous failures. Longer diagnostic test intervals as specified in the datasheet has to be considered separately in safety parameter calculations, see IEC 61508-2, 7.4.9.4.
- Beta Factor: If the components/component is used in safety relevant architecture with a HFT ≥ 1 a beta factor has to be considered in safety loop calculations. The beta factor for the component is initial (β_{int}). To estimate the final beta factor for a specific application the effects of the architecture have to be considered. Thus, the beta factor has to be calculated individual according IEC 61508-6, table D.5.
- Beta Factor Diagnostics: β_D is the fraction of dangerous common cause failures if the components/component is used in safety relevant architectures, which can be detected by diagnostic tests.
  see IEC 61508-6, table B1.

Verification of SIL-capability (examples)

The SIL verification consists of two steps:

- Step (1) = quantitative verification by calculation of the pfh-value / pfd-value depending from the defined Proof Test Interval and used architecture. The max. reachable SIL for the calculated safety loop within the component is used can be estimated according IEC 61508-1 table 2 (for low demand operation) or table 3 (for high demand operation)
- Step (2) = qualitative verification based on the architectural information of the set of components/component according route 1_H, the qualitative max. SIL is defined in IEC 61508-2, 7.4.4.2.

The final achievable SIL is the minimum resulting SIL-value of step (1) and step (2): MIN {(1) ; (2)}. The final achievable SIL is only relevant for the final safety loop not for a single component used in the safety loop.

IEC 61508-2 permits SIL 3 applications with an architecture with HFT = 0 according to route 1H in case of SFF > 90% for type A components. From technical safety point of view, this can only be accepted if the overall system risk is higher using a redundant safety related architecture in comparison using a single channel architecture. Using non-redundant safety related architectures for SIL 3 application is in general evaluated as insufficient. For SIL 3 application a safety related architecture with HFT ≥ 1 is highly recommended.

Further remarks using safety relevant parameters

- If operating medium is required (oil, air, etc.), failure rate of operating medium is not considered in the safety related parameter shown in this datasheet.
- Failure Rates considering diagnostic measures with DC > 0 may only be used if diagnosis is installed in the application with sufficient quality.
- Common cause failures, which can occur using the analyzed component in architectures, have to be considered by the user in safety loop calculations.
- If the subsystem is used in application with architectures, e.g. in a 1oo2 architecture, a beta-factor for the subsystem derived from βint acc. IEC 61508-6, table D.5 has to be considered in the safety loop calculation of the application.

INGENIEURBÜRO URBAN – Dipl.-Ing. J. Urban
Öffentl. Bestellung u. Vereidigung ◆ Zeichen für Sachverstand ◆ Unabhängigkeit ◆ Unparteilichkeit
Publicly certified ◆ The mark of quality in the expert profession ◆ Independence ◆ Impartiality
Certificatión pública ◆ Señal de competencia ◆ Independencia ◆ Imparcialidad